IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRIC OF ILLINOIS
EASTERN DIVISION

RODNEKA PERRY and SAMANTHA YOUNG, individually, and on behalf of all others similarly situated,	)	
Plaintiff,	)	**Case No. 1:23-cv-03383**
v.	)	
AMAZON LOGISTICS, INC., AMAZON.COM, INC., AMAZON.COM SERVICES, LLC f/k/a AMAZON.COM, LLC, and AMAZON WEB SERVICES, INC.	)	
Defendants.	)	

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Rodneka Perry ("Plaintiff Perry") and Samantha Young ("Plaintiff Young") (collectively "Plaintiffs"), individually and on behalf of all others similarly situated (the "Class"), bring the following Class Action Complaint ("Complaint") pursuant to FRCP 23 and against (1) Amazon Logistics, Inc., (2) Amazon.com, Inc., (3) Amazon.com Services, LLC f/k/a Amazon.com, LLC, and, (4) Amazon Web Services, Inc. ("AWS"), collectively, ("Amazon" or "Defendants") to redress and curtail each Defendant's unlawful collection, use, storage, and disclosure of Plaintiffs' and other similarly situated individuals' sensitive and proprietary biometric identifiers and biometric information ("biometric data"). Plaintiffs allege as follows upon personal knowledge as to themselves, their own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

NATURE OF THE ACTION

1. Amazon.com, Inc. and Amazon.com Services, LLC, commonly known as "Amazon," is a leading multinational technology company, specializing in e-commerce, cloud-based servicing, streaming and artificial intelligence. It is considered one of the "Big Four" technology companies, alongside Google, Apple, and Facebook.

2. Amazon Logistics, Inc., is a subsidiary of Amazon.com, Inc. and provides the fulfillment and delivery infrastructure for Amazon.com, Inc. through applications, including, but not limited to Amazon Flex. Amazon Flex is a job service platform with a corresponding application that provides an opportunity for individuals to accept assignments and deliver packages on behalf of Amazon Logistics, Inc. or Amazon.com, Inc. using their own vehicles.

3. AWS is a subsidiary of Amazon.com, Inc. and one of the largest platforms and providers for cloud computing services.

4. In September 2018, Plaintiff Perry downloaded the Amazon Flex application, created an account, and started work as a delivery driver in the Greater Chicago area and continues to do so until the present.

5. In December 2019, Plaintiff Young downloaded the Amazon Flex application, created an account, and started work as a delivery driver in the Greater Chicago area and continues to do so until the present.

6. Through Amazon Flex, Plaintiffs accept jobs and deliver Amazon packages, Prime Now household items, and Amazon Fresh groceries to customers in the Greater Chicago area using their own vehicles.

7. In mid-2019 Amazon Flex installed a feature where, before Plaintiffs or anyone else can accept work and start delivering packages, the user is required to scan his or her face using their mobile device for identity verification purposes.

8. Any Amazon Flex user, including Plaintiffs, must have their facial geometry collected and stored by Amazon as a requirement for them to deliver Amazon's packages.

9. Amazon Flex admits as much in the FAQ section of its application where it states:

> "To use the Amazon delivery application, Amazon requires that users provide a photo to help us identify them. Using this photo, we may create a facial scan or similar biometric identifier, which we refer to as 'Biometric Information.'"[1]

10. However, Amazon fails to secure Amazon Flex users' informed written consent before collecting, storing, and disseminating their biometric identifiers and biometric information.

11. Since approximately 2016, Amazon has been using Artificial Intelligence ("AI") machine-learning image and video recognition systems, including Amazon Rekognition.

12. Rekognition is an image-recognition technology that Amazon uses itself and markets and sells to businesses, governmental entities, and other third parties through AWS. According to AWS's own FAQ, the most common use cases for Rekognition include: "Searchable Image Library, Face-Based User Verification, Sentiment Analysis, Facial Recognition, and Image Moderation."[2]

13. Amazon captures the image data of Plaintiffs and other Illinois Amazon Flex users which are then shared with Amazon software programs, including but not limited to Rekognition, to identify and detect and to enhance their own systems and technology, including the Rekognition system itself.

---

[1] *Amazon Flex – FAQs* (last visited April 14, 2023), https://flex.amazon.com/faq
[2] *Amazon Rekognition – FAQs* (last visited July 21, 2022), https://aws.amazon.com/rekognition/faqs/?nc=sn&loc=7

14. Upon information and belief, Amazon requires its Amazon Flex users to take and upload pictures of themselves into the application and uses associated facial recognition software, including but not limited to Rekognition, in order to verify the users' identities before allowing them to proceed with their Amazon Flex shift.

15. Defendant AWS's associated facial recognition software collects and captures, stores and uses biometric identifiers, namely scans of an individual's facial geometry.

16. Facial geometry and other biometrics are unique and personal identifiers that cannot be changed. 740 ILCS § 14/5(c).

17. Critically, it is unclear how long each Defendant retains the biometric identifiers and information derived from the capturing of Plaintiffs' and other Amazon Flex users' faces.

18. Recognizing the need to protect its citizens' right of control over their biometric data, Illinois enacted the Biometric Information Privacy Act ("BIPA"), 740 ILCS § 14/1, *et seq.*, specifically to regulate companies that collect, store, and use Illinois citizens' biometrics, such as facial geometry scans. 740 ILCS § 14/5.

19. Notwithstanding the clear and unequivocal requirements of the law, Amazon knowingly disregards Plaintiffs' and other similarly situated users' statutorily protected privacy rights and unlawfully collects, obtains, stores, disseminates, and uses Plaintiffs' and other similarly situated users' biometric data in violation of BIPA. Specifically, Defendants violated and continue to violate BIPA because they did not and continue not to:

a. Properly or adequately inform Plaintiffs and others similarly situated in writing that biometric identifiers or biometric information are being collected, obtained or stored, as required by BIPA;

b. Properly or adequately inform Plaintiffs and others similarly situated in writing of the specific purpose and length of time for which her facial scans and other biometric identifiers or biometric information were being collected, obtained, stored, and used, as required by BIPA;

c. Develop and adhere to a BIPA-compliant publicly available retention schedule and guidelines for permanently destroying Plaintiffs' and others similarly situated facial scans and other biometric identifiers or biometric information, as required by BIPA;

d. Obtain a written release from Plaintiffs and others similarly situated to collect, obtain, capture, or otherwise obtain their facial scans and other biometric identifiers or biometric information, as required by BIPA; and,

e. Obtain consent from Plaintiffs and others similarly situated to disclose, redisclose, or otherwise disseminate their facial scans and other biometric identifiers or biometric information to a third party, as required by BIPA.

20. Accordingly, Plaintiffs, on behalf of themselves as well as the putative Class, seeks an Order: (1) declaring that Amazon's conduct violates BIPA; (2) requiring Amazon to cease the unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiffs and the putative Class.

PARTIES

21. Plaintiff Perry is a natural person and at all relevant times was a resident of the State of Illinois.

22. Plaintiff Young is a natural person and at all relevant times was a resident of the State of Illinois.

23. Defendant Amazon.com, Inc. is a Delaware corporation that is registered to do business in Illinois.

24. Defendant Amazon.com Services, LLC is a Delaware corporation that is registered to do business in Illinois.

25. Defendant Amazon Web Services, Inc. is a Delaware corporation that is registered to do business in Illinois.

26. Defendant Amazon Logistics, Inc. is a Delaware corporation that is registered to do business in Illinois.

JURISDICTION AND VENUE

27. On April 17, 2023, this Class Action Complaint was originally brought pursuant to 735 ILCS § 5/2-209 in the Circuit Court of Cook County for violations of the Illinois Biometric Information Privacy Act (740 ILCS 14/1 *et seq*.) which Amazon removed to this Court on May 30, 2023. *See* Dkt. #1.

28. This is Plaintiffs' First Amended Class Action Complaint for violations of the Illinois Biometric Information Privacy Act (740 ILCS 14/1 *et seq*.) brought pursuant to Fed. R. Civ. P. 23 seeking statutory and actual damages.

29. Venue is proper in this Court because a substantial amount of the acts and omissions giving rise to this action occurred within this judicial district.

30. This Court has jurisdiction over this dispute pursuant to 28 U.S.C. § 1332 because Plaintiff and the proposed class members are all residents of Illinois, Defendant is domiciled outside of Illinois and the amount in controversy exceeds $75,000.

31. This Court has jurisdiction over this dispute pursuant to the Class Action Fairness Act ("CAFA") because the prospective class includes over 100 people and the amount in controversy exceeds $5,000,000.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act.

32. In the early 2000s, major national corporations started using Chicago and other locations in Illinois to test "new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS

§ 14/5(c). Given its relative infancy, an overwhelming portion of the public became weary [sic] of this then-growing yet unregulated technology. *See* 740 ILCS § 14/5.

33. In late 2007, a biometrics company called Pay by Touch, which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions—including at retail grocery stores—filed for bankruptcy. That bankruptcy alarmed the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records—which, like other unique biometric identifiers, can be linked to people's sensitive financial and personal data—could now be sold, distributed, or otherwise shared through the bankruptcy proceedings to third parties without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who used the company's fingerprint scanners were completely unaware the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to Pay by Touch, and that their unique biometric identifiers could now be sold to unknown third parties. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276, p. 249.

34. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS § 14/5.

35. Additionally, to ensure compliance, BIPA provides that, for each violation, the prevailing party may recover $1,000 or actual damages, whichever is greater, for negligent violations and $5,000, or actual damages, whichever is greater, for intentional or reckless violations. 740 ILCS § 14/20.

36. BIPA is an informed consent statute that achieves its goal by making it unlawful for a company to, among other things, collect, capture, purchase, receive through trade, or

otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first:

a. Informs the subject in writing that a biometric identifier or biometric information is being collected, obtained, stored, and used;

b. Informs the subject in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, obtained, stored, and used; and

c. Receives a written release executed by the subject of the biometric identifier or biometric information.

See 740 ILCS § 14/15(b).

37. Biometric identifiers include facial scans, retina and iris scans, voiceprints, scans of hands, and fingerprints. *See* 740 ILCS § 14/10. Biometric information is defined separately to include any information based on an individual's biometric identifier that is used to identify an individual. *Id.*

38. BIPA establishes standards for how companies must handle biometric identifiers and biometric information. *See, e.g.*, 740 ILCS § 14/15(c)-(d). For example, BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for such disclosure. *See* 740 ILCS § 14/15(d)(1).

39. BIPA requires companies to develop and comply with a written policy—made available to the public—establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting such identifiers or information has been satisfied, or within three years of the individual's last interaction with the company, whichever occurs first. 740 ILCS § 14/15(a).

40. The Illinois legislature enacted BIPA due to the increasing use of biometric data in financial and security settings, the general public's hesitation to use biometric information, and—

significantly—the unknown ramifications of biometric technology. Biometrics are biologically unique to the individual and, once compromised, an individual is at a heightened risk for identity theft and left without any recourse. 740 ILCS § 14/5.

41. BIPA provides individuals with a private right of action, protecting their right to privacy regarding their biometrics as well as protecting their rights to know the precise nature for which their biometrics are used and how they are being stored and ultimately destroyed. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, store, use, and disseminate biometrics and creates a private right of action for lack of statutory compliance. 740 ILCS § 14/20.

42. Plaintiffs, like the Illinois legislature, recognize how imperative it is to keep biometric information secure. Biometric information, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

II. Amazon Violates the Biometric Information Privacy Act.

43. Each Defendant failed to take note of the shift in Illinois law governing the collection, use, storage, and dissemination of biometric data and continues to collect, store, use, and disseminate Amazon Flex users' biometric data in violation of BIPA.

44. In 2019, Amazon faced a similar lawsuit alleging that Amazon's "Alexa" devices retained minor users' voice prints and information without proper consent in violation of BIPA. There, Amazon was accused by guardians of minors of unlawful collection, use, storage and disclosure of minor users' biometric data through the use of its "Alexa" devices and voice printing system. Between 2019 – 2023, at least twenty other similar lawsuits have since been brought against Amazon entities, including AWS, alleging BIPA violations from their improper collection

of individuals' biometric identifiers and information and their improper use of said data to train and enhance Rekognition.[3]

45. Despite these prior accusations and all Defendants' knowledge of BIPA, here, Amazon captures and scans Amazon Flex users' biometric identifiers, particularly their facial geometry, through Amazon Flex's identity verification checks, and uploads and stores their data

[3] *See Trio v. Amazon Web Services, Inc.*, Case No 1:23-CV-01389, filed March 6, 2023, in the Northern District of Illinois (removed from the Circuit Court of Cook County Illinois, Case No. 2023-CH-00544); *See Redd v. Amazon Web Services, Inc.*, Case No. 1:22-CV-06779, filed Dec. 2, 2022, in the Northern District of Illinois (removed from the Circuit Court of Cook County, Illinois, with Case No. 2022-CH-08721)*; See Dorian v. Amazon Web Services, Inc.*, Case No. 2:22-CV-00269, filed March 7, 2022, in the Western District of Washington; *See Reid v. Amazon.com, Inc. et al.*, Case No. 1:21-CV-06010, filed Nov. 9, 2021, in the Northern District of Illinois; *See Mayhall v. Amazon Web Services, Inc. et al.*, Case No. 2:21-CV-04173, filed Oct. 29, 2021, in the Western District of Washington; *See Svoboda v. Amazon, Inc., et al*, Case No. 1:21-CV-05336, filed Oct. 7, 2021, in the Northern District of Illinois (removed from the Circuit Court of Cook County, Illinois, with Case No. 2021-CH-04516); *See Schaeffer v. Amazon.com, Inc. et al.,* Case No. 3:21-CV-01080, filed Aug. 31, 2021, in the Southern District of Illinois (removed from the Circuit Court of Madison County, Illinois, under Case No. 2021-C-000876); *See Flores et al., v. Amazon, Inc. et al.,* Case No. 1:21-CV-04064, filed Aug. 2, 2021, in the Northern District of Illinois (case in other court: Washington Western, 2:21-CV-00873); *Cooper v. Amazon, Inc. et al.,* Case No. 2:21-CV-00915, filed Jul. 8, 2021, in the Western District of Washington (electronically transferred on Aug. 30, 2021, to the Northern District of Illinois, as Case No. 1:21-CV-04633; *See B.H. v. Amazon.com, Inc.*, Case No. 1:21-CV-03169, filed Jun. 11, 2021, in the Northern District of Illinois (removed from the Circuit Court of Cook County, Illinois, Case No. 2021-CH-02330); *See Rosati v. Amazon.com, Inc.*, Case No. 2:21-CV-00409, filed March 26, 2021, in the Western District of Washington (removed from the Superior Court of Washington for King County, Case No. 21-2-03591 SEA); *See Bond v. Amazon, Inc.*, Case No. 1:21-CV-01578, filed Jan. 28, 2021, in the 16th Judicial Circuit Court, Kane County, Illinois; *See Jerinic v. Amazon.com, Inc.*, Case No. 1:20-CV-06485, filed Oct. 20, 2020, in the Northern District of Illinois (removed from the Circuit Court of Cook County, Illinois, Case No. 2020-CH-06036); *See Vance v. Amazon.com, Inc.*, Case No. 2:20-CV-01084, filed July 14, 2020, in the Western District of Washington; *See Ragsdale v. Amazon Web Services, Inc.*, Case No. 1:20-CV-00560, filed Jan. 24, 2020, in the Northern District of Illinois (removed from the Circuit Court of Cook County, Illinois, case no. 2109-CH-013251); *See McGoveran v. Amazon Web Services, Inc.* Case No. 3:20-CV-00031, filed Jan. 8, 2020, in the Southern District of Illinois (removed from the Circuit Court of Madison County, Illinois, Case No. 2019-L-001786) (*McGoveran et al v. Amazon Web Services, Inc. et al.*, Case No. 1:20-CV-01399, filed Oct. 16, 2020, in the District of Delaware); *See Hryniewick v. Amazon Web Services, Inc.,* Case No. 1:19-CV-07569, filed Nov. 15, 2019, in the Northern District of Illinois (removed from the Circuit Court of Lake County, Illinois, Case No. 2019-CH-00001155); *See Adamsky et al v. Amazon.com, Inc. et al.*, Case No. 2:19-CV-01214, filed Aug. 2, 2019, in the Western District of Washington; *See Wilcosky v. Amazon.com, Inc. et al.*, Case No. 1:19-CV-05061, filed July 26, 2019, in the Northern District of Illinois (removed from the Circuit Court of Cook County, Illinois, Case No. 2019-CH-07777); *See Williams v. Inpax Shipping Solutions*, Case No. 2018-CH-02307, filed Feb. 21, 2018, in the Circuit Court of Cook County, Illinois.

on Amazon's networked databases for use with Amazon's facial detection and recognition technology and software, including but not limited to Rekognition.

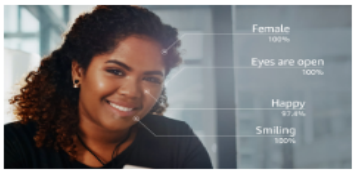
46. Amazon uses the biometric identifiers and information of Amazon Flex users from image data captured by Amazon Flex to identify users and to train and enhance the Rekognition system.

47. This is done through one of Rekognition's main features which is its ability to detect and analyze faces from still images or videos and compare them with other faces detected from other images. From these images, Rekognition can provide information including but not limited to "…facial landmarks such as the position of eyes, and detected emotions such as happy or sad."[4] Once an image containing a face is provided to Rekognition, it "detects the face in the image, analyzes the facial attributes of the face, and then returns a percent confidence score for the face and facial attributes that are detected in the image." *See* Figures 1 and 2 below, showing screenshots from Amazon's AWS Rekognition website and Developer Guide.

Face compare and search

Determine the similarity of a face against another picture or from your private image repository.

Learn more »



Face detection and analysis

Detect faces appearing in images and videos and recognize attributes such as open eyes, glasses, and facial hair for each.

Learn more »

Figure 1.

[4] *Amazon Rekognition - Developer Guide* (last visited July 18, 2022), https://docs.aws.amazon.com/rekognition/latest/dg/rekognition-dg.pdf#what-is

Detecting and analyzing faces

Amazon Rekognition can detect faces in images and videos. This section covers non-storage operations for analyzing faces. With Amazon Rekognition, you can get information about where faces are detected in an image or video, facial landmarks such as the position of eyes, and detected emotions (for example, appearing happy or sad). You can also compare a face in an image with faces detected in another image.

When you provide an image that contains a face, Amazon Rekognition detects the face in the image, analyzes the facial attributes of the face, and then returns a percent confidence score for the face and the facial attributes that are detected in the image.

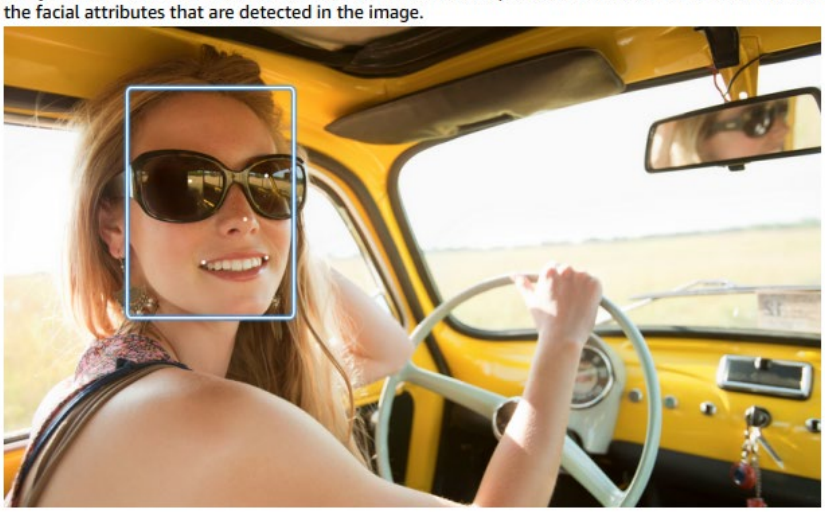


Figure 2.

Searching faces in a collection

Amazon Rekognition can store information about detected faces in server-side containers known as collections. You can use the facial information that's stored in a collection to search for known faces in images, stored videos, and streaming videos. Amazon Rekognition supports the IndexFaces operation. You can use this operation to detect faces in an image and persist information about facial features that are detected into a collection. This is an example of a *storage-based* API operation because the service persists information on the server.

To store facial information, you must first create (CreateCollection) a face collection in one of the AWS Regions in your account. You specify this face collection when you call the `IndexFaces` operation. After you create a face collection and store facial feature information for all faces, you can search the collection for face matches. To search for faces in an image, call SearchFacesByImage. To search for faces in a stored video, call StartFaceSearch. To search for faces in a streaming video, call CreateStreamProcessor.

Figure 3.

Note
The service doesn't persist actual image bytes. Instead, the underlying detection algorithm first detects the faces in the input image, extracts facial features into a feature vector for each face, and then stores it in the collection. Amazon Rekognition uses these feature vectors when performing face matches.

You can use collections in a variety of scenarios. For example, you might create a face collection to store scanned badge images by using the `IndexFaces` operation. When an employee enters the building, an image of the employee's face is captured and sent to the `SearchFacesByImage` operation. If the face match produces a sufficiently high similarity score (say 99%), you can authenticate the employee.

48. (Rekognition is also able to store the information from these scans ("facial metadata") into databases which it can search through to compare faces. *See* Figure 3 above, showing a screenshot from Amazon's AWS Rekognition Developer Guide.

49. Each Defendant fails to adequately inform Amazon Flex users that it is collecting, obtaining or storing biometric data; fails to adequately inform Amazon Flex users of the specific purposes and duration for which it collects and obtains their sensitive biometric data and that the purpose of Amazon's biometric data collection is to identify and detect users and to train Rekognition; fails to obtain written releases from Amazon Flex users before collecting or obtaining their sensitive biometric data; and fails to inform Amazon Flex users that it discloses their sensitive biometric data to AWS, amongst Defendants, to other Amazon entities, and to other, currently unknown, third parties, which, *inter alia*, host and/or analyze the biometric data.

50. Each Defendant also fails to establish a BIPA-compliant written, publicly available policy identifying its retention schedule and guidelines for permanently destroying Amazon Flex users' biometric data when the initial purpose for collecting or obtaining their biometrics has been satisfied or within three years of the individual's last interaction with any of the Defendants, whichever occurs first, as required by BIPA.

51. The Pay by Touch bankruptcy that catalyzed the passage of BIPA, as well as the recent data breaches, highlights why such conduct—where individuals are aware they are providing a biometric identifier, but not aware of to whom or for what purposes they are doing so—is dangerous. That bankruptcy spurred Illinois citizens and legislators into realizing how crucial it is for individuals to understand when providing biometric identifiers, such as facial scans, who exactly is collecting their biometric data, where the biometric data will be transmitted and for what purposes, and how long the biometric data will be retained. Each Defendant disregards these

obligations and Amazon Flex users' statutory rights and instead unlawfully collects, stores, uses, and disseminates users' biometric identifiers and information, all without receiving the informed written consent required by the BIPA. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276.

52. Each Defendant lacks BIPA-compliant retention schedules and guidelines for permanently destroying Plaintiffs' and the putative Class's biometric data and has not and will not destroy Plaintiffs' and the putative Class's biometric data as required by BIPA.

53. Each Defendant fails to inform Amazon Flex users what will happen to their biometric data in the event Amazon merges with another company or ceases operations, or what will happen in the event the third parties that receive, store, and/or manage Plaintiffs' and the putative Class's biometric data from Amazon cease operations.

54. These violations of BIPA raise a material risk that Plaintiffs' and the putative Class's biometric data will be unlawfully accessed by third parties.

55. By and through the actions detailed above, Amazon knew of, yet disregarded Plaintiffs' and the putative Class's legal rights in violation of BIPA.

III. Plaintiffs' Experiences

56. In September 2018, Plaintiff Perry downloaded the Amazon Flex application on her mobile device and created an account to begin working as a delivery driver using her own vehicle.

57. In 2019, Plaintiff Young downloaded the Amazon Flex application on her mobile device and created an account to begin working as a delivery driver using her own vehicle.

58. Plaintiffs deliver Amazon packages, household items from Prime Now, and even groceries from Amazon Fresh.

59. When signing up for a delivery shift or "time block," Plaintiffs are directed to drive to one of Amazon's local fulfillment centers. Since mid-2019, once the Amazon Flex application confirms their location that they have arrived at the fulfillment center, the application will prompt an identity check. This identity check requires Plaintiffs to take and upload a picture of themselves. *See* Figures 4 and 5 below, showing screenshots from the Amazon Flex application's identity verification prompt.

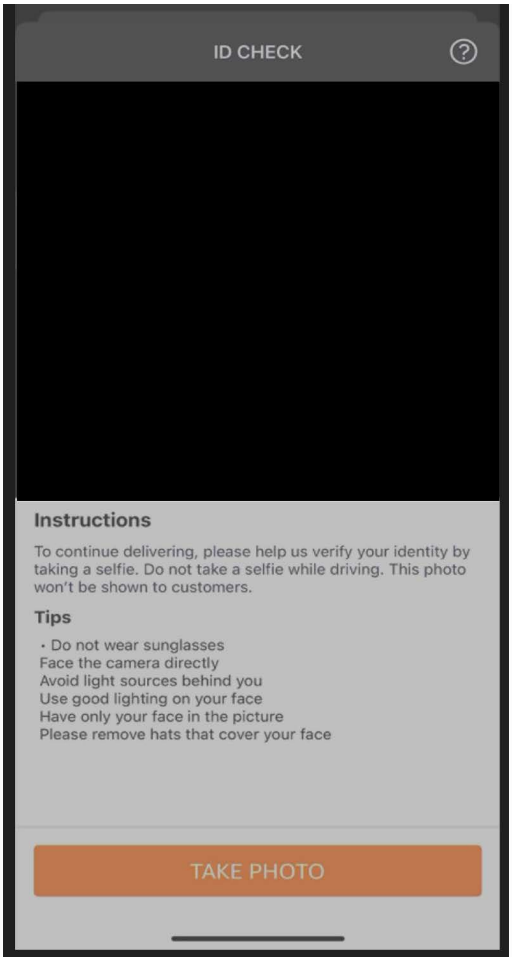


Figure 4.

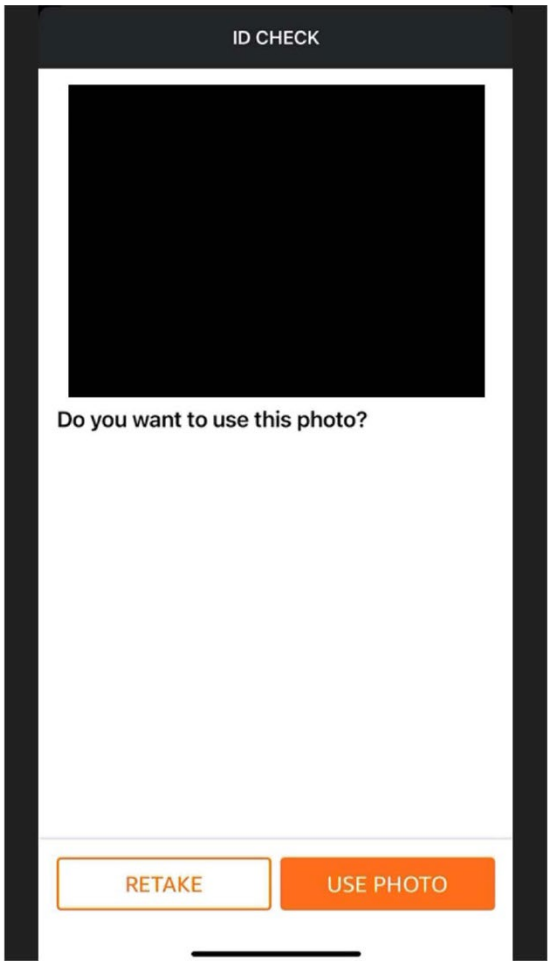


Figure 5.

60. Next, Plaintiffs are required to scan their government-issued I.D. at a kiosk at the fulfillment center location. Amazon Flex then uses facial recognition software to verify their identity before allowing Plaintiffs to proceed with the job of delivering packages. This process scans Plaintiffs' and other users' facial geometry and derives uniquely identifying biometric information to compare to the biometric information Amazon Flex already has stored. *See* Figures 6 and 7 below, showing screenshots from the Amazon Flex application's identity verification prompt.

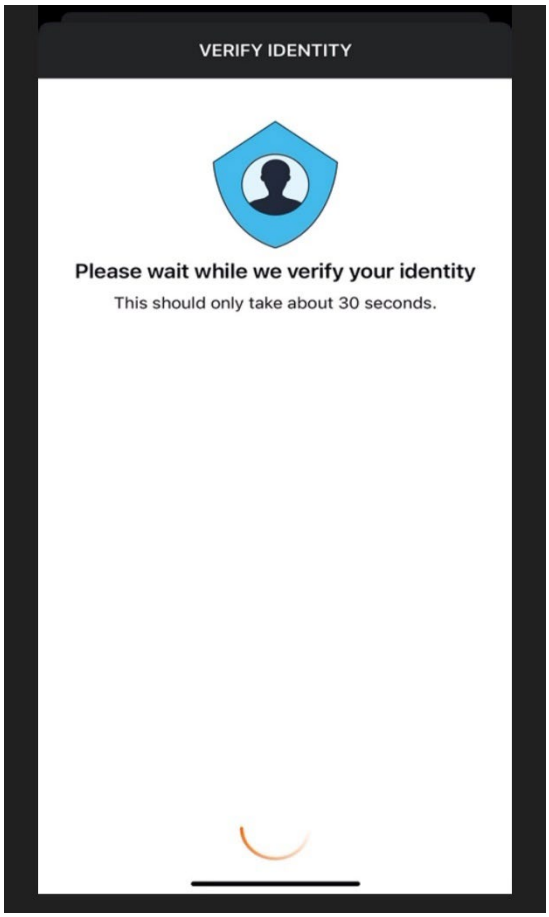


Figure 6.

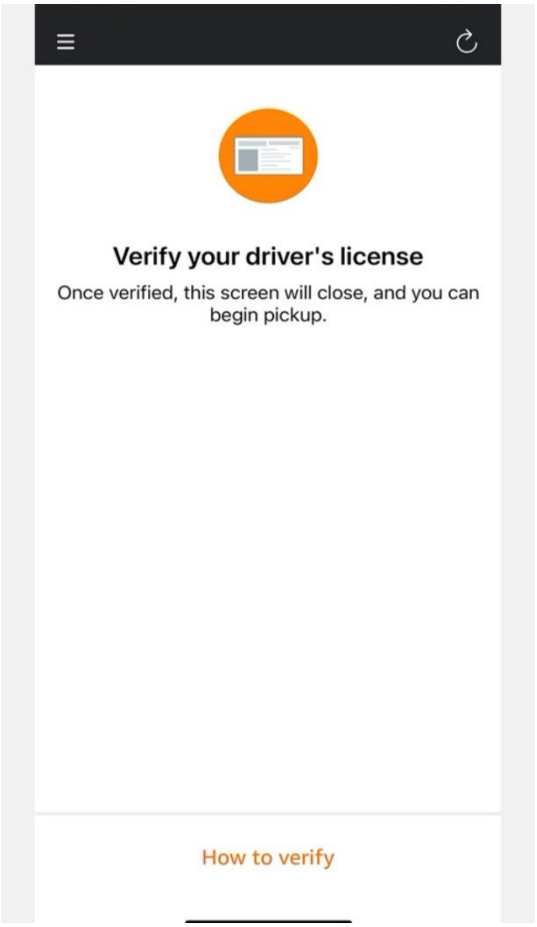


Figure 7.

61. Each Defendant collected, captured, or otherwise obtained scans of Plaintiffs' facial geometry and other biometric identifiers by facial recognition technology software, including but not limited to Rekognition, through the Amazon Flex application whenever Plaintiffs and other Amazon Flex users signed up to deliver packages.

62. Amazon disclosed Plaintiffs' sensitive biometric data to other Amazon entities, amongst Defendants, to AWS, and to other, currently unknown, third parties, which, *inter alia*, host and/or analyze the biometric data.

63. Amazon never (1) adequately informed Plaintiffs in writing or otherwise that it was collecting, obtaining or storing her biometric data or of the specific purpose(s) and length of time for which her biometric data was being collected; (2) received a written release from Plaintiffs to collect, obtain, store, or use her biometric data; (3) developed or adhered to a BIPA-compliant publicly available retention schedule and guidelines for permanently destroying Plaintiffs' biometric data; (4) or obtained Plaintiffs' consent for any disclosure or dissemination of their biometric data to third parties.

64. Plaintiffs have never been informed by any Defendant of the specific limited purposes or length of time for which Amazon collects, captures, obtains, stores, uses, and/or disseminates their biometric data.

65. Plaintiffs have never seen, been made aware of, or been able to find, view, or access a BIPA-compliant publicly available biometric data retention policy developed by any Defendant, nor have they ever seen, been made aware of, or been able to find, view, or access any policies regarding whether any Defendant will ever permanently delete their biometric data.

66. No BIPA-compliant retention schedules or destruction guidelines relating to biometric data were in Plaintiffs' onboarding materials when they began working for Amazon Flex.

67. No BIPA-compliant retention schedules or destruction guidelines relating to biometric data are currently available to Plaintiffs or other Amazon Flex users on a company intranet.

68. No BIPA-compliant retention schedules or destruction guidelines relating to biometric data are available on the Amazon Flex application.

69. Plaintiffs have not been provided with nor ever signed a written release allowing Amazon to collect, capture, obtain, store, use, or disseminate their biometric data.

70. Plaintiffs have been continuously and repeatedly exposed to the risks and harmful conditions created by each Defendant's violations of BIPA alleged herein.

71. No amount of time or money can compensate Plaintiffs if their biometric data has been compromised by the intentional, reckless, and/or negligent procedures through which Amazon captures, stores, uses, and disseminates their and the putative Class's biometric data. Moreover, Plaintiffs would not have provided their biometric data to any Defendant if they had known Defendants would retain such information for an indefinite period of time without their consent.

72. A showing of actual damages is not necessary to state a claim under BIPA. *See Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 40 ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an "aggrieved" person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act").

73. As Plaintiffs are not required to allege or prove actual damages to state a claim under BIPA, they seek statutory damages under BIPA as compensation for the injuries caused by Defendants. *Rosenbach*, 2019 IL 123186, ¶ 40.

CLASS ALLEGATIONS

74. Pursuant to Fed. R. Civ. P. 23, Plaintiffs brings claims on their own behalf, and as representatives of all other similarly situated individuals, pursuant to BIPA, 740 ILCS § 14/1, *et seq.*, to recover statutory penalties, prejudgment interest, attorneys' fees and costs, and other damages owed for the violations described herein.

75. Under Rule 23, Plaintiffs seek certification of the following Class:

> All individuals who used the Amazon Flex application in the State of Illinois and who had their facial geometry scans or any other biometric identifiers and/or biometric information, collected, captured, received, or otherwise obtained, maintained, stored, used, disclosed, disseminated by any Defendant during the applicable statutory period.

76. Excluded from the Class are Defendants' officers and directors, and any judge, justice, or judicial officials presiding over this matter and their immediate families.

77. This action is properly maintained as a class action under Rule 23 because:

A. The Class is so numerous that joinder of all members is impracticable;

B. There are questions of law or fact that are common to the Class;

C. Plaintiffs' claims are typical of the claims of the Class; and,

D. Plaintiffs will fairly and adequately protect the interests of the Class.

Numerosity

78. There are at least tens of thousands of putative Class members. The exact number of Class members can easily be determined from Defendants' records.

Commonality

79. There is a well-defined commonality of interest in the substantial questions of law and fact concerning and affecting the Class in that Plaintiffs and all members of the Class have been harmed by each Defendant's failure to comply with BIPA. The common questions of law and fact include, but are not limited to the following:

A. Whether any Defendant collected, captured, received, or otherwise obtained, maintained, stored, used, disclosed or disseminated Plaintiffs' and the Class's biometric identifiers or biometric information;

B. Whether any Defendant informed Plaintiffs and the Class that it was collecting or storing their biometric identifiers and biometric information;

C. Whether any Defendant properly informed Plaintiffs and the Class of the specific purpose and duration for which Defendants were collecting, using, storing, and disseminating their biometric identifiers or biometric information;

D. Whether any Defendant properly obtained a written release (as defined in 740 ILCS § 14/10) to collect, use, store, and disseminate Plaintiffs' and the Class's biometric identifiers or biometric information;

E. Whether any Defendant has disclosed, redisclosed, or otherwise disseminated Plaintiffs' and the Class's biometric identifiers or biometric information;

F. Whether any Defendant developed a BIPA-compliant written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of its last interaction with the individual, whichever occurs first;

G. Whether any Defendant complied with any such written policy (if one exists);

H. Whether any Defendant's violations of BIPA have raised a material risk that Plaintiffs' and the putative Class's biometric data will be unlawfully accessed by third parties;

I. Whether any Defendant used Plaintiffs' and the Class's biometric identifiers, including scans of their facial geometry, to identify them;

J. Whether any Defendant used Plaintiffs' and the Class's biometric identifiers, including scans of their facial geometry to enhance facial recognition technology including Rekognition;

K. Whether the violations of BIPA were committed negligently; and,

L. Whether the violations of BIPA were committed intentionally or recklessly.

80. Plaintiffs anticipate Defendants will raise defenses that are common to Plaintiffs and the Class.

Adequacy

81. Plaintiffs will fairly and adequately protect the interests of all members of the Class, and there are no known conflicts of interest between Plaintiffs and class members. Plaintiffs, moreover, have retained experienced counsel who are competent in the prosecution of complex litigation and who have extensive experience serving as class counsel.

Typicality

82. The claims asserted by Plaintiffs are typical of the Class members they seek to represent. Plaintiffs have the same interests and suffered from the same unlawful practices as the Class.

83. Upon information and belief, there are no other Class members who have an interest in individually controlling the prosecution of his or her individual claims, especially in light of the relatively small value of each claim. However, if any such Class member should become known, s/he can "opt out" of this action pursuant to Rule 23.

Predominance and Superiority

84. The common questions identified above predominate over any individual issues, which will relate solely to the quantum of relief due to individual class members. A class action is superior to other available means for the fair and efficient adjudication of this controversy because

individual joinder of the parties is impracticable. Class action treatment will allow a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of effort and expense if these claims were brought individually. Moreover, as the damages suffered by each class member are relatively small in the sense pertinent to class action analysis, the expenses and burden of individual litigation would make it difficult for individual class members to vindicate their claims.

85. Additionally, important public interests will be served by addressing the matter as a class action. The cost to the court system and the public for the adjudication of individual litigation and claims would be substantially more than if claims are treated as a class action. Prosecution of separate actions by individual class members would create a risk of inconsistent and varying adjudications, establish incompatible standards of conduct for Defendants and/or substantially impair or impede the ability of class members to protect their interests. The issues in this Action can be decided by means of common, class-wide proof. In addition, if appropriate, the Court can and is empowered to fashion methods to efficiently manage this Action as a class action.

FIRST CAUSE OF ACTION

Violation of 740 ILCS § 14/15(a): Failure to Institute, Maintain, and Adhere to Publicly Available Retention Schedule and Destruction Guidelines

86. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

87. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention—and, importantly, deletion—policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent destruction of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually destroy the biometric information. *See* 740 ILCS § 14/15(a).

88. All Defendants fail to comply with these BIPA mandates.

89. Defendant Amazon.com, Inc. is a Delaware corporation that is registered to do business in Illinois, and therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

90. Defendant Amazon.com Services, LLC is a Delaware corporation that is registered to do business in Illinois, and therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

91. Defendant Amazon Web Services, Inc. is a Delaware corporation that is registered to do business in Illinois, and therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

92. Defendant Amazon Logistics, Inc. is a Delaware corporation that is registered to do business in Illinois, and therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

93. Plaintiffs and the putative Class are individuals who have had their "biometric identifiers" and "biometric information" collected by Defendants, as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

94. All Defendants failed to publish a BIPA-compliant, publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. *See* 740 ILCS § 14/15(a).

95. All Defendants lack BIPA-compliant retention schedules and guidelines for permanently destroying Plaintiffs' and the Class's biometric data and have not and will not destroy Plaintiffs' or the Class's biometric data when the initial purpose for collecting or obtaining such

data has been satisfied or within three years of the Plaintiffs' and Class members' last interaction with any Defendant, whichever occurs first.

96. On behalf of themselves and the putative Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring each Defendant to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

SECOND CAUSE OF ACTION

Violation of 740 ILCS § 14/15(b): Failure to Obtain Informed Written Consent and Release Before Collecting or Obtaining Biometric Identifiers or Information

97. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

98. BIPA requires companies to obtain informed written consent from individuals before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information." 740 ILCS § 14/15(b).

99. All Defendants fail to comply with these BIPA mandates.

100. Defendant Amazon.com, Inc. is a Delaware corporation that is registered to do business in Illinois, and therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

101. Defendant Amazon.com Services, LLC is a Delaware corporation that is registered to do business in Illinois, and therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

102. Defendant Amazon Web Services, Inc. is a Delaware corporation that is registered to do business in Illinois, and therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

103. Defendant Amazon Logistics, Inc. is a Delaware corporation that is registered to do business in Illinois, and therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

104. Plaintiffs and the putative Class are individuals who have had their "biometric identifiers" and "biometric information" collected by Defendants, as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

105. All Defendants systematically and automatically collected, captured, or otherwise obtained Plaintiffs' and the putative Class's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS § 14/15(b)(3).

106. No Defendant has ever adequately informed Plaintiffs and the putative Class in writing that their biometric identifiers and/or biometric information were being collected, captured, or otherwise obtained, nor did any Defendant ever inform Plaintiffs and the putative Class in writing of the specific purpose(s) and length of term for which their biometric identifiers and/or

biometric information were being collected, stored, used, and disseminated as required by 740 ILCS § 14/15(b)(1)-(2).

107. By collecting, capturing, or otherwise obtaining Plaintiffs' and the putative Class's biometric identifiers and biometric information as described herein, all Defendants violated Plaintiffs' and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS § 14/1, *et seq.*

108. On behalf of themselves and the putative Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring each Defendant to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

THIRD CAUSE OF ACTION

Violation of 740 ILCS § 14/15(d): Disclosure or Dissemination of Biometric Identifiers and Information Before Obtaining Consent

109. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

110. BIPA prohibits private entities from disclosing or disseminating a person's or customer's biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS § 14/15(d)(1).

111. All Defendants fail to comply with this BIPA mandate.

112. Defendant Amazon.com, Inc. is a Delaware corporation that is registered to do business in Illinois, and therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

113. Defendant Amazon.com Services, LLC is a Delaware corporation that is registered to do business in Illinois, and therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

114. Defendant Amazon Web Services, Inc. is a Delaware corporation that is registered to do business in Illinois, and therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

115. Defendant Amazon Logistics, Inc. is a Delaware corporation that is registered to do business in Illinois, and therefore, qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

116. Plaintiffs and the putative Class are individuals who have had their "biometric identifiers" and "biometric information" collected by Defendants, as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

117. All Defendants systematically and automatically disclosed, redisclosed, or otherwise disseminated Plaintiffs' and the Class's biometric identifiers and/or biometric information to AWS, amongst Defendants, to other Amazon entities, and to other, currently unknown, third parties, which, *inter alia*, host and/or analyze the biometric data as separate private entities without first obtaining the consent required by 740 ILCS § 14/15(d)(1).

118. By disclosing, redisclosing, or otherwise disseminating Plaintiffs' and the Class's biometric identifiers and biometric information as described herein, each Defendant violated

Plaintiffs' and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS § 14/1, *et seq.*

119. On behalf of themselves and the putative Class, Plaintiff seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring each Defendant to comply with BIPA's requirements for the collection, storage, use, and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

PRAYER FOR RELIEF

Wherefore, Plaintiffs respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff Perry and Young as Class Representatives, and appointing Stephan Zouras, LLP, Michael L. Fradin and James L. Simon as Class Counsel;

B. Declaring that each Defendant's actions, as set forth above, violate BIPA;

C. Awarding statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each non-willful violation of BIPA pursuant to 740 ILCS § 14/20(1);

D. Declaring that each Defendant's actions, as set forth above, were intentional and/or reckless or, in the alternative, were negligent;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class, including an Order requiring each Defendant to collect, store, use, and disseminate biometric identifiers and/or biometric information in compliance with BIPA and to delete and destroy any biometric identifiers and information previously collected from Class members;

F. Awarding Plaintiffs and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3);

G. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable; and,

H. Awarding such other and further relief as equity and justice may require.

Date: August 15, 2023

Respectfully Submitted,

/s/Mohammed A. Rathur

Ryan F. Stephan
Catherine Mitchell
Mohammed A. Rathur
STEPHAN ZOURAS, LLP
222 W. Adams Street, Suite 2020
Chicago, Illinois 60606
Telephone: (312) 233-1550
Facsimile: (312) 233-1560
rstephan@stephanzouras.com
cmitchell@stephanzouras.com
mrathur@stephanzouras.com

s/ *Michael L. Fradin*
Michael L. Fradin, Esq.
FRADIN LAW
8401 Crawford Ave. Ste. 104
Skokie, IL 60076
Telephone: 847-986-5889
Facsimile: 847-673-1228
Email: mike@fradinlaw.com

By: /s/ *James L. Simon*
James L. Simon (*pro hac vice* forthcoming)
SIMON LAW CO.
11 ½ N. Franklin Street
Chagrin Falls, OH 44022
Telephone: (216) 816-8696
Email: james@simonsayspay.com

Counsel for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on August 15, 2023, I filed the attached with the Clerk of the Court using the electronic filing system which will send such filing to all attorneys of record.

/s/ Mohammed A. Rathur